EXHIBIT B

John R. Strand

Owner / Senior Security Analyst
Black Hills Information Security

John Strand is Senior Security Analyst/Principal of Black Hills Information Security. Before BHIS, John started the practice of computer security with Accenture Consulting in the areas of intrusion detection, incident response, and vulnerability assessment/penetration testing. John then moved to Northrop Grumman specializing in DCID 6/3 PL3-PL5 (multi-level security solutions), security architectures, and program certification and accreditation.

John teaches and authors classes for the SANS institute and Security Weekly. John was the course author and instructor for SEC464: Hacker Guard: Security Baseline Training for IT Administrators and Operations with Continuing Education, and the co- author for SEC580: Metasploit Kung Fu for Enterprise Pen Testing and SANS 504: Hacker Techniques and Incident Response.

He is currently the lead author of Antisyphon's Pay What You Can training.

He also teaches SEC504: Hacker Techniques, Exploits, and Incident Handling; SEC560: Network Penetration Testing and Ethical Hacking; for the SANS institute. He is also the author of Offensive Countermeasures: The Art of Active Defense. John has presented for multiple organizations and 'cons' including the FBI, NASA, NSA, RSA and DefCon. John is the host of Hack Nacked TV with Security Weekly and enjoys co-hosting Security Weekly. John is one of the minds and leaders behind Offensive Counter Measures and Active defense, which he hopes will change the security industry for the better.

Experience and Work History

Black Hills Information Security, Owner **Present**

-Penetration testing for DoD/SCI Programs, banks, hospitals and e-commerce customers
-HIPPA Security consulting
-Security Architecture Reviews
-Vulnerability Assessments
-Computer Forensics

Northrop Grumman, Information Assurance Security Engineer **Aug 2004 to July 2007**

-Responsible for working within and leading teams for engineering and review of all security related aspects of complex Secret, Top Secret, and SCI systems.
-Corporate computer forensics utilizing Forensic Toolkit, and HELIX on over 50 systems.
-Created test procedures for systems of various Protection Levels (PL1-PL4). Test procedures correspond with Government computer security requirements.
-Performing vulnerability assessments utilizing the latest hacker tools and techniques.
-Job duties relate heavily to the DCID 6/3, and DIACAP requirements to prepare systems for a full audit and review across multiple Top Secret and SCI programs.
-ISSO Responsibilities
-Job duties require Top Secret SCI clearance, which requires a 10 year history Single Scope Background Investigation (SSBI).
-Current Polygraph

Accenture Consulting, Specialist/Security Tech Level 3 **January 2001 to Aug 2004**

Incident Handling Lead

-Developed Incident Handling procedures adopted by the Department of the Interior Mineral Resource Management (MRM).
-Served as main point of contact/coordinator for multiple cyber security incidents directing the actions of over twenty individuals across the United States.

-Advised Minerals Management Service Information Technology directors on proper incident response actions.
-Development of MRM's Incident handing capability was key to removing court ordered restrictions against the Department of the Interior.

Technical Vulnerability Assessment Specialist

-Developed Technical Vulnerability Assessment procedures adopted by the Department of the Interior, Mineral Resource Management.
-Assessed and recommended the current tools and techniques set used by MRM.
-Utilize Technical Vulnerability Assessment tools and techniques on an up-to-date and ongoing basis.

Security Monitoring Specialist

-Developed Security Monitoring procedures adopted by the Department of the Interior Mineral Resource Management.
-Developed the current security logging system used by MRM. This system utilizes Microsoft Operations Manager, Aelita Event Admin, and LANGuard Security Event Logging Manager.
-Trained the current security team at MRM to analyze and respond to potentially damaging Security events.
-Assisted in developing the current Intrusion Detection Systems (IDS) used by MRM.
-Trained the current security team at MRM to analyze respond to IDS alerts.
-Development of MRM's Security Monitoring capability was key to removing court ordered restrictions against the Department of the Interior.

Project Lead

-Lead for the Technical Vulnerability Assessment, System/IDS log review, and Incident Handling Development Projects.
-Coordinated both consulting and client actions required to complete the above mentioned projects.
-Received approval for the above mentioned projects from Government client leads.

Oracle Database Management

-Assisted with user and database object access and permissions.
-Created and maintained database objects using DBA techniques.

Education, Certifications and Skills

Denver University, Masters of Applied Science in Computer Information Systems **June 2006**

University of Wyoming, Bachelor of Science in Political Science **December 2000**

Certifications

-Certified Information System Security Profession (CISSP) - CISSP #38328, January 2003
-SANS Global Information Assurance Certification GCIH Incident Handling and Hacker Techniques and Exploits – Certified Gold GCIH #343 Sept 2002, Sept 2004
-SANS Global Information Assurance Certification GCFW Firewalls, Perimeter Protection and VPNs – Certified Gold GCFW #468 March 2004

Teaching Experience

-SANS Instructor for GCIH: Incident Handling and Hacker Techniques and Exploits
-SANS Instructor for GPEN: Network Penetration Testing

BLACK HILLS INFORMATION SECURITY

-SANS Local Mentor for CISSP Preparation
-Adjunct Professor for Colorado Technical University
-Adjunct Professor for Denver University

Technical Skills

Intrusion Detection
- -Implementation and managing of Snort, and Cisco Secure IDS, Cisco MARS, OSSIM, and honeypot/honeynet technologies.
- -Reading of IDS logs for signs of system compromise, and weeding out false positives.

System Base-lining
- -Developing and implementing of system base-lining procedures. These procedures monitor systems monthly for unauthorized system modifications.
- -Tools utilized: Tripwire, Nmap, Hot Fix Checker, fc, SYSDIFF, RPM, LANGuard Security Scanner, and Exporter.

Firewall Technology
- -Firewall concepts, implementation and maintenance
- -Netfilter, PIX, Cybergaurd, and Checkpoint Firewall technology

Penetration Testing
- -Developing and implementing penetration testing procedures. These skills include external and internal penetration testing.
- -Tools utilized: Metasploit, Nessus, Whisker, Nmap, Hping, Netcat, Windump, TCPDump, ISS Internet Scanner, ISS Database Scanner, John the Ripper, PWDump3e, L0phtcrack, Scapy, and other hacker techniques and exploits.

Cyber Forensics
- -Developing and implementing of forensic procedures as part of a six-step incident handling process. This includes identifying how a system was compromised and assessing the extent of the damage.
- -Tools utilized: Ethereal, Windump, FTK, TCPDump, Autopsy, dd, FTimes, Snort, wipe, DumpEVT, Mcafee, Norton, and eTrust InoculateIT Antivirus programs and other Windows and UNIX/Linux command line utilities.

Incident Handling
- -Responding to breaches of security. This includes determining how an intruder or malicious code entered a network and insuring that it does not infect the system again.

Forensics
- -Reviewing corporate date for possible compromise.
- -Tools utilized: Forensic Toolkit, HELIX, Autopsy, dd, standard Unix command like tools.

TCP/IP
- -Reading raw TCP/IP data
- -Tools utilized: Ethereal, Windump, TCPDump